



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/975,410	10/10/2001	Jukka Vialen	930.339-US-W1	1295
32294	7590	11/19/2004	EXAMINER	
SQUIRE, SANDERS & DEMPSEY L.L.P. 14TH FLOOR 8000 TOWERS CRESCENT TYSONS CORNER, VA 22182			CHOU, ALBERT T	
			ART UNIT	PAPER NUMBER
			2662	

DATE MAILED: 11/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/975,410

Applicant(s)

VIALEN ET AL.

Examiner

Albert T. Chou

Art Unit

2662

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 October 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,6-9,17 and 19-24 is/are rejected.
- 7) ☒ Claim(s) 2-5,10-16 and 18 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 10 October 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 11-13-04.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Applicant is required to provide the following documents which are listed in applicant's Information Disclosure Statement but were not submitted for this application:

Krayem-Nevoux R et al: "Payphone Service For Third Generation Mobile Systems," Proceedings of the Global Telecommunications Conference, Vol.-, 29 November 1993, pgs 1708-1712.

Von Bernd Friedrichs: "Authentische Und Zuverlassige Mobilkommunikation fur sicherheitsrelevante Anwendungen. Teil II: Systemarchitektur Und Einbettung in GSM; Vol. 49, No.3/04, 1 March 1995, pgs 48-57.

Claim Rejections - 35 USC § 112

2. Claims 6 and 7 recite the limitation "said algorithm". There is insufficient antecedent basis for this limitation in the claim.
3. Claims 9 and 20 recite the limitation "the integrity algorithm". There is insufficient antecedent basis for this limitation in the claim.
4. Claim 17 recites the limitation "said input values". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 112

5. Claims 1, 19, 22, 23 and 24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite ("some of said values being the same for said different channels") for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1, 6, 8, 9, 17, 19, 20, 21, 22, 23 and 24 are rejected under 35 U.S.C. 102(b) as being anticipated by 3GPP TS 33.102 V3.9.0 (2001-06) Release 1999 hereinafter 3GPP.

Regarding claims 1 and 19, 3GPP teaches (Figure 14, page 29) local authentication and connection set-up between MS and SRNC (method of communication between a first node and a second node) comprising the step of (Figure 14, pages 29-30) generating MAC-I (step of calculating an integrity output). The input parameters to the integrity algorithm f9 (Figure 16, page 33) are IK, COUNT-I, MESSAGE, DIRECTION and FRESH (said integrity output being calculated from a plurality of values). The signaling MESSAGE itself (page 35) is with the radio bearer identify, RB 0-4 (page 34), which is appended in front of the message (at least one of

said values comprising the information relating to the identity of said channel, each channel having a different identity). 3GPP further teaches (Figure 14, pages 29-30) that SRNC attaches the MAC-I to the RRC message Security control mode command and sends it to MS (step of transmitting information relating to the integrity output from one of said nodes to the other).

Regarding claim 6, 3GPP teaches that the input parameters to the integrity algorithm f9 are the integrity key (IK), the integrity sequence number (COUNT-I), a random value generated by the network side (FRESH), the direction bit DIRECTION and the signaling data MESSAGE (Figure 16, page 33).

Regarding claim 8, 3GPP teaches that the signaling MESSAGE itself is with the radio bearer identify. However, the radio bearer identity is not transmitted with the message (page 35).

Regarding claim 9, 3GPP teaches that SRNC attaches the MAC-I to the RRC message Security control mode command and sends it to MS (Figure 14, pages 29-30).

Regarding claim 17, 3GPP teaches that the input parameters, IK, COUNT-I, MESSAGE, DIRECTION and FRESH, are inputs to the integrity algorithm f9 for calculating MAC, the output (Figure 16, page 33).

Regarding claims 20, 3GPP teaches (Figure 14, page 29) local authentication and connection set-up between MS and SRNC (method of communication between a first node and a second node) comprising the step of (Figure 14, pages 29-30) generating MAC-I (step of calculating an integrity output). The input parameters to the integrity algorithm f9 (Figure 16, page 33) are Integrity Key (IK), COUNT-I, MESSAGE,

Art Unit: 2662

DIRECTION and FRESH (calculating an integrity output using a plurality of values, one of said values being an integrity key). 3GPP teaches (page 34) that there may be one IK (IKcs) for CS connections and one IK (IKps) for PS connections (each of said channels having a different integrity key). 3GPP further teaches (Figure 14, pages 29-30) that SRNC attaches the MAC-I to the RRC message Security control mode command and sends it to MS (step of transmitting information relating to the integrity output from one of said nodes to the other).

Regarding claim 21, 3GPP teaches (Figure 15, pages 30-31) that SRNC periodically performs a local authentication procedure between MS and SRNC. The SRNC is monitoring the COUNT-C value associated to each radio bearer. The procedure is triggered whenever any of these values reaches a critical checking value (triggering an authentication procedure). 3GPP further teaches (page 30) that the granularity of these checking values and the values themselves are defined by the visited network (calculating a desired number of integrity parameters)

Regarding claims 22, 3GPP teaches (Figure 14, pages 29-30) SRNC comprising means for generating MAC-I (step of calculating an integrity output). The input parameters to the integrity algorithm f9 (Figure 16, page 33) are IK, COUNT-I, MESSAGE, DIRECTION and FRESH (said integrity output being calculated from a plurality of values). The signaling MESSAGE itself (page 35) is with the radio bearer identify, RB 0-4 (page 34), which is appended in front of the message (at least one of said values comprising the information relating to the identity of said channel, each channel having a different identity). 3GPP further teaches (Figure 14, pages 29-30) that

SRNC attaches the MAC-I to the RRC message Security control mode command and sends it to MS (means for transmitting information relating to the integrity output from said node to said further node).

Regarding claims 23, 3GPP teaches (Figure 14, pages 29-30) SRNC comprising means for generating MAC-I (step of calculating an integrity output). The input parameters to the integrity algorithm f9 (Figure 16, page 33) are IK, COUNT-I, MESSAGE, DIRECTION and FRESH (said integrity output being calculated from a plurality of values). The signaling MESSAGE itself (page 35) is with the radio bearer identify, RB 0-4 (page 34), which is appended in front of the message (at least one of said values comprising the information relating to the identity of said channel, each channel having a different identity). 3GPP further teaches (Figure 14, pages 29-30) SRNC comprising means that at the reception of the response message from MS, the SRC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I (means for comparing information relating to the integrity output calculated by said node with a value calculated by the further node).

Regarding claims 24, 3GPP teaches the integrity algorithm f9 (Figure 16, page 33) comprising means for generating MAC-I (means for calculating an integrity output). The input parameters to the integrity algorithm (Figure 16, page 33) are IK, COUNT-I, MESSAGE, DIRECTION and FRESH (said integrity output being calculated from a plurality of values). The signaling MESSAGE itself (page 35) is with the radio bearer identify, RB 0-4 (page 34), which is appended in front of the message (at least one of

Art Unit: 2662

said values comprising the information relating to the identity of said channel, each channel having a different identity).

Allowable Subject Matter

7. Claims 2, 3, 4, 5, 10, 11, 12, 13, 14, 15, 16 and 18 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Albert T. Chou whose telephone number is 571-272-6045. The examiner can normally be reached on 8:30 - 17:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Kizooou can be reached on 571-272-3088. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AC
Albert Chou
November 12, 2004

Chau T. Nguyen
CHAU NGUYEN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600